CLAIMS

What is claimed is:

1. Virus and intrusion protection apparatus for use with a computer comprising:

a dedicated network board exclusively for external communications with the World-Wide-Web, email and other external networks; and

a switch connecting the dedicated network board and a main core of the computer wherein when the switch is open, the main core of the computer is disconnected from the dedicated network board and the World-Wide-Web, email and other external networks.

2. The apparatus according to Claim 1, wherein the dedicated network board includes:

a central processing unit (CPU);

cache;

memory; and

communications ports and software for communicating with the World-Wide-Web, email and other external networks.

3. The apparatus according to Claim 2, wherein the dedicated network board further includes a modem.

4. The apparatus according to Claim 1, further comprising a modem coupled to the dedicated network board.

5. The apparatus according to Claim 1, wherein the dedicated network board further comprises:

temporary storage media for storing information from the World-Wide-Web;

email software for sending and receiving email;

web access programs for communicating with the World-Wide-Web; and

inspection software for emails and world-wide-web communications.

6. The apparatus according to Claim 5, wherein the email software comprises a booby tray address book and the main core comprises an email address book of email recipients.

7. The apparatus according to Claim 5, wherein the dedicated network board further comprises: flush and reset software for flushing and resetting the temporary storage media upon detection of a virus.

8. The apparatus according to Claim 1, wherein when transferring data from the dedicated network board to the main core, a connection to the World-Wide-Web, the email or the other external network is severed, the computer commands the switch to close and thereafter data is transferred from the temporary storage media to storage media of the main core.

9. A method for protecting a computer from a virus, hacker or worm comprising the steps of:

providing a dedicated network access board exclusively for communications with World-Wide-Web, email and other external networks;

connecting a main core of the computer to the dedicated network access board via a switch; and

opening the switch to connect the World-Wide-Web, the email or the other external networks to the network board via a network connection and disconnecting the World-Wide-Web, the email and the other external networks from the main core of the computer to protect the computer from the virus, the worms, or the hackers.

10. The method according to claim 9, wherein the method further includes the steps of:

when data is desired from the main core of the computer:

severing the network connection to the World-Wide-Web, the email or the other external network;

closing the switch to establish a connection between the dedicated network board and the main core of the computer; and

transferring files from the dedicated network board to a storage media of the main core.

11. The method according to claim 9, further comprising the steps of:

commanding the computer to connect to the World-Wide-Web, the email or the other external network; and

in response to the commanding step, automatically opening the switch to disconnect the main core from the World-Wide-Web, the email or the other external network.

12. The method according to claim 9, further comprising the steps of:

when transferring clean data obtained from the World-Wide-Web, the email or the other external network to the main core:

severing the network connection;

closing the switch; and

transfer files from the temporary storage media to the core's storage media.

13. Virus and intrusion protection apparatus for use with a computing unit comprising:

means dedicated to exclusive external communications with World-Wide-Web; and

means for switching the dedicated external communications means and a main core of the computing wherein when the switching means is open, the main core of the computing unit is disconnected from the dedicated external communications means and the World-Wide-Web while communications commence with the World-Wide-Web.

14. The apparatus according to Claim 13, wherein the computing unit is a computer.

15. The apparatus according to Claim 14, wherein the dedicated external communications means includes:

a central processing unit (CPU);

cache;

memory; and

communications ports and software for communicating with the World-Wide-Web.

16. The apparatus according to Claim 15, wherein the dedicated external communications means further comprises:

temporary storage media for storing information from the World-Wide-Web;

email software for sending and receiving email;

web access programs for communicating with the World-Wide-Web; and

inspection software for emails and world-wide-web communications.

17. The apparatus according to Claim 16, wherein the email software comprises a booby tray address book and the main core comprises an email address book of email recipients.

18. The apparatus according to Claim 17, wherein the dedicated external communications means further comprises: flush and reset software for flushing and resetting the temporary storage media upon detection of a virus.

19. The apparatus according to Claim 18, wherein when transferring data from the dedicated external communications means to the main core, a connection to the World-Wide-Web is severed, the computer commands the

switching means to close and thereafter data is transferred from the temporary storage media to storage media of the main core.

20. The apparatus according to Claim 13, wherein:

the computing unit is a network server; and

the dedicated external communications means includes:

a central processing unit (CPU);

cache;

memory; and

communications ports and software for communicating with the World-Wide-Web.